

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICES ASSIGNED CALL
NUMBERS: (865) 209-████ WITH
INTERNATIONAL MOBILE EQUIPMENT
IDENTITY ("IMEI") NUMBER
35348103046877; (865) 250-████ WITH
IMEI NUMBER 3549160929271; AND (423)
215-████ WITH IMEI NUMBER
452716086922130, STORED AT PREMISES
CONTROLLED BY CELLCO
PARTNERSHIP d.b.a. VERIZON
WIRELESS

Case No. 3:20-mj-2126

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, J. Jason Pack being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephones assigned call numbers: (865) 209-████ with IMEI number 35348103046877; (865) 250-████ with IMEI number 35491609292716; and (423) 215-████ with IMEI number 452716086922130 ("the SUBJECT PHONES"), that is stored at premises controlled by Verizon Wireless, a wireless telephone service provider headquartered at One Verizon Way, Basking Ridge, New Jersey, 07920. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Verizon Wireless to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information

described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

3. Simultaneously with the Application submitted herewith, I am applying for a search warrant for Apple iCloud records for the account associated with identifier badtrucking@icloud.com. The facts set forth in the Affidavit in support of that Application for iCloud records and information is incorporated fully by reference herein.

4. There is probable cause to believe that records and information captured by Verizon in their normal course of business will be present at the premises to be search and will provide information pertaining to Miller's and the victim's use of the SUBJECT PHONES, during the course of the offenses and substantiating the victim's disclosures. Through subpoena returns, Verizon confirmed it was the provider of service for the SUBJECT PHONES for the dates pertinent to this investigation. It is reasonable to believe, based on photographs recovered through forensic examination, the victim was with Miller and historical cell site and tower records currently in the custody of Verizon Wireless will be relevant to the investigation and substantiate the victim's allegations and the location of the offenses.

5. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate

information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

6. Based on my training and experience, I know that Verizon Wireless can collect cell-site data about the SUBJECT PHONES. I also know that wireless providers such as Verizon Wireless typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes. On 4/29/2020, your affiant caused a preservation letter for the above-mentioned accounts to be served on Verizon Wireless.

7. Based on my training and experience, I know that Verizon also collects per-call measurement data, which Verizon also refers to as the “real-time tool” (“RTT”). RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

8. Based on my training and experience, I know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers in their normal

course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as Verizon Wireless typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONES' user or users.

9. Based on the facts set forth in this affidavit, there is probable cause to believe that Everett Eugene Miller ("Miller") has transported a minor in interstate commerce with intent for the minor to engage in sexual activity for which a person can be charged with a criminal offense in violation 18 U.S.C. § 2423(a) and there is probable cause to search for the information described in Attachment A for evidence and instrumentalities of these crimes, as further described in Attachment B.

AUTHORIZATION REQUEST

10. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

11. I further request that the Court direct Verizon Wireless to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Verizon Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

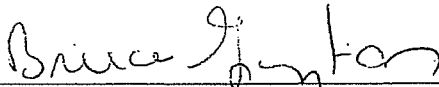
12. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,



J. Jason Pack
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 15, 2020



UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephones assigned call numbers:

1. (865) 209-████ with International Mobile Equipment Identity Number 35348103046877
2. (865) 250-████ with International Mobile Equipment Identity Number 35491609292716
3. (423) 215-████ International Mobile Equipment Identity Number 452716086922130

("the Accounts"), that are stored at premises controlled by Celco, d.b.a Verizon Wireless ("the Provider"), headquartered at One Verizon Way, Basking Ridge, New Jersey, 07920.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period June 30, 2019 to February 3, 2020:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, usernames, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long-distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received as well as per-call measurement data (also known as the “real-time tool” or “RTT” data).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 2423(a) involving Everett Eugene Miller during the period June 30, 2019 through February 3, 2020.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE
902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Verizon Wireless, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Verizon Wireless. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Verizon Wireless, and they were made by Verizon Wireless as a regular practice; and
- b. such records were generated by Verizon Wireless' electronic process or system that produces an accurate result, to wit:
 1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Verizon Wireless in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Verizon Wireless, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature